Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

# FERMAT'S LAST THEOREM AND THE ORIGIN AND NATURE OF THE THEORY OF ALGEBRAIC NUMBERS.

BY L. E. DICKSON.

## Introduction.

Of the many interesting and important facts about whole numbers which were discovered by Fermat nearly three centuries ago, all have since been proved with one exception, the so-called last theorem of Fermat, which asserts that $x^n + y^n = z^n$ has no integral solutions different from zero when $n > 2$. Fermat stated that he had found a truly remarkable proof. His scientific reputation is such that one can at most doubt the accuracy of his proof. This challenge problem has received attention from many mathematicians of the highest ability, including Euler, Legendre, Gauss, Abel, Sophie Germain, Dirichlet, Kummer and Cauchy.

The problem is important chiefly on account of its relation to the history of mathematics. The publication of a complete proof would deprive the problem of its chief claim to attention for its own sake, but not its claim to historical importance. For, the study of this challenge problem and the general law of reciprocity of higher residues led Kummer to invent his ideal numbers, out of which grew the general theory of algebraic numbers, one of the most important branches of modern mathematics. As remarked by Hensel,* it would seem at first sight to be a misfortune that Fermat did not have space on the margin of his copy of Diophantus to write down his proof; but further reflection leads one to regard this circumstance as one fortunate for the development of science; for, while we might perhaps have possessed a complete proof of Fermat's theorem, not in itself so important, we would certainly not possess Kummer's ideal theory which grew up solely out of attempts to prove that theorem. Kummer devoted twenty of his best years to the development of his ideal numbers, holding always before himself as goal the complete proof of Fermat's last theorem and the general reciprocity law, and declaring that he would probably have abandoned his theory of ideal numbers, in spite of its success, if he had known another method of proving that theorem and law. We, to whom Kummer's theory appears as the foundation stone of arithmetic, are of another opinion; we would on the contrary thank Fermat's problem that through it the genius of a Kummer was so forcibly directed that we now possess the theory of ideals. Gauss had previously investigated the special algebraic integers $a + bi$ in connection with the law of reciprocity of biquadratic residues.

---

* Abhand. Geschichte Math. Wiss., 29, 1910, p. 19, p. 30.

Part I of this paper is devoted to the early history of Fermat's last theorem and to a summary of the more important results concerning it which have been proved without the theory of algebraic numbers. The papers which treat Fermat's theorem by means of algebraic numbers are reserved for Part III. The points of view needed for this final part are developed in a very elementary way in Part II.

But the chief aim of Part II (which may be read independently of Parts I and III) is to enable the general reader to obtain, with a minimum of effort, a clear insight into the origin, nature and use of ideals. The exposition is limited to the concrete, but typical, case of a particular quadratic domain, thereby avoiding the algebraic complications which arise for the general domain.

Contrary to the intuition of Lamé, Cauchy, Wantzel and initially of Kummer himself, the numbers involving a single algebraic irrationality do not obey the laws of arithmetic; the restoration of those laws by the introduction of the ideals was one of the chief scientific triumphs of the last century.

The writer is indebted to H. S. Vandiver and H. H. Mitchell for suggestions on the manuscript and proof sheets.

## Part I.

### Early History of Fermat's Last Theorem. Results Obtained Without the Use of the Theory of Ideals.

1. **Sum of two cubes not a cube.** A defective proof was given before 972 by the Arab Alkhodjandi.* The Arab Beha-eddin† (1547–1622) listed among the problems remaining unsolved from former times that to divide a cube into two cubes. P. Fermat‡ proposed the problem to find two cubes whose sum is a cube to Sainte-Croix, September, 1636, to Frenicle, May, 1640, to the mathematicians of England and Holland, August 15, 1657, and later§ declared that the problem is impossible.

---

* Cf. F. Woepcke, Atti Accad. Pont. Nuovi Lincei, 14, 1860–1, 301.

† Essenz der Rechenkunst von Mohammed Beha-eddin ben Alhossain . . . von G. H. F. Nesselmann, 1843, p. 55. French transl. by A. Marre, Nouv. Ann. Math., 5, 1846, 313; ed. 2, Rome, 1864.

‡ Oeuvres de Fermat, 2, p. 65, p. 195, p. 346; 3, p. 287, p. 313.

§ Oeuvres, 2, p. 376, p. 433, letter to Digby, Apr. 7, 1658, to Carcavi, Aug., 1659.

The proof by Euler[*] was reproduced by Legendre.[†] Gauss[‡] gave a proof by use of a cube root of unity.

2. **Sum or difference of two biquadrates never a square.** Each of these propositions implies that $x^4 + y^4 = z^4$ is impossible in integers not zero. Leonardo Pisano[§] gave an incomplete proof of the fact that $x^2 + y^2$ and $x^2 - y^2$ are not both squares and implied the related theorem that the area of a right triangle with rational sides is never a perfect square. P. Fermat's[||] proof of the latter theorem is of special interest as it illustrates his famous method of infinite descent and as it is the only instance of a detailed proof left by him. The proof shows incidentally that the difference of two biquadrates is not a square. An analogous proof, doubtless due to Fermat, was published by Frenicle de Bessy,[¶] who proved also that no square is a sum of two biquadrates. In a MS. dated Dec. 29, 1678, Leibniz[**] proved that the area of a primitive right triangle with integral sides is not a square; hence $v^4 - w^4$ is not a square, as shown by the area of the triangle formed from $v^2$ and $w^2$ by Diophantus's rule.[††] Euler[‡‡] gave simple proofs that $a^4 + b^4 \neq c^2$ if $ab \neq 0$; $a^4 - b^4 \neq c^2$ if $b \neq 0, b \neq a$; these proofs were reproduced by Legendre.[§§]

3. **Fermat's theorem from elementary standpoints.** About 1637, P. Fermat,[||||] commenting on Diophantus II, 8 (to solve $x^2 + y^2 = a^2$), stated that "it is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into two powers of like degree; I have discovered a truly remarkable proof which this margin is too small to contain."

Claude Jaquemet[¶¶] (1651–1729) gave a false proof, thinking that

---

[*] Algebra, 2, 1770, art. 243, pp. 509–16; French tr., 1774, 2, pp. 343–51; Opera Omnia (1), 1, 484–9.

[†] Théorie des nombres, 1798, pp. 407–8. Cf. ed. 3, 1830, art. 653.

[‡] Posthumous MS., Werke, 2, 387–390.

[§] Tre Scritte Inediti de L. Pisano, Rome, 1854, p. 98. Scritti di L. Pisano, Rome, vol. 2, 1862, p. 272. Cf. Genocchi, Annali di Sc. Mat. Fis., 6, 1855, 131–2, 293–310.

[||] Fermat's marginal notes on his copy of Bachet's edition (1621) of Diophantus's Arithmetica. Oeuvres de Fermat, 1, 1891, p. 340; 3, 1896, p. 271.

[¶] Traité des Triangles Rectangles en Nombres, Paris, 1676, pp. 101–6; Mém. Acad. Sc. Paris, 1666–1699, p. 5, éd. 1729, p. 178.

[**] Math. Schriften (ed. C. I. Gerhardt), vol. 7, 1863, pp. 120–5.

[††] The triangle formed from $m$, $n$ has the sides $2mn$, $m^2 - n^2$, $m^2 + n^2$.

[‡‡] Comm. Acad. Petrop., 10, 1747 (1738), pp. 125–134; Comm. Arith. Coll., 1, pp. 24–34. Same in Euler's Algebra, 2, 1770, p. 418; 1774, pp. 242–54; Opera omnia (1), 1, 1911, p. 437.

[§§] Théorie des nombres, 1798, p. 404; ed. 2, 1808; Maser, 1893, 2, p. 5.

[||||] Diophanti Alexandri Arith. libri sex, ed. S. Fermat, Tolosae, 1670, p. 61. Oeuvres de P. Fermat, 1, p. 291; 3, p. 241.

[¶¶] Ms. in the Bibliothèque Nationale de Paris, published by A. Marre, Bull. Bibl. Storia Sc. Mat. Fis., 12, 1879, 886–894. Cf., pp. 565–8.

$p - r$ cannot divide $pq - rs$. Sophie Germain,* in her first letter to Gauss, Nov. 21, 1804, stated that she could prove that

$$x^n + y^n + z^n = 0 \tag{1}$$

is impossible if $n + 1$ is a prime of the form $8k + 7$.

P. Barlow† considered integers $x$, $y$, $z$ relatively prime in pairs, each not zero, and satisfying [1], where $n$ is an odd prime. Then

$$\phi(x, y) = \frac{x^n + y^n}{x + y} = x^{n-1} - x^{n-2}y + \cdots + y^{n-1} \tag{2}$$

is either prime to $x + y$ or has with it the greatest common divisor $n$, according as $z$ is not or is divisible by $n$, a result due to Jacquemet. In the respective cases, Barlow deduced [4] and [5]. His attempt to prove the impossibility of [1] involved the error that a sum of fractions in their lowest terms is not an integer if the denominator of each fraction has a factor not dividing all the remaining denominators.

N. H. Abel‡ stated that solutions of [1] are of the form [4], [5] or

$$2x = c^n + n^{n-1}(a^n + b^n), \qquad 2y = c^n - n^{n-1}(a^n + b^n),$$
$$2z = -c^n - n^{n-1}(a^n - b^n).$$

But the third case is unnecessary. He stated that [1] is impossible when any of the quantities $x$, $y$, $z$, $x - y$, $x - z$, $y - z$, $x^{1/n}$, $y^{1/n}$, $z^{1/n}$ are primes.

A. M. Legendre,§ after remarking that the French Academy of Sciences had offered one of its prizes for a proof of Fermat's last theorem, but without awarding the prize, developed some results which he credited to Sophie Germain. First, let no one of the relatively prime numbers $x$, $y$, $z$ satisfying [1] be divisible by the odd prime $n$. Then $x + y$ and the expression [2] are relatively prime and their product equals $(-z)^n$. Hence we may set

$$\begin{array}{lll} y + z = a^n, & \phi(y, z) = \alpha^n, & x = -a\alpha, \\ z + x = b^n, & \phi(z, x) = \beta^n, & y = -b\beta, \\ x + y = c^n, & \phi(x, y) = \gamma^n, & z = -c\gamma. \end{array} \tag{3}$$

---

* Oeuvres phil., 1879, p. 298. Cinq lettres de S. Germain à Gauss, 1880. Archiv Math. Phys., 65, 1880, Litt. Bericht, pp. 27–31.

† Appendix to English transl. of Euler's Algebra. Proof "completed" in Jour. Nat. Phil. Chem. Arts, 27, 1810, p. 193 and reproduced in Barlow's Theory of Numbers, London, 1811, 160–9. Changing the sign of $x$, we shall write his equation in the form [1].

‡ Oeuvres, 2, 1881, 254–5, letter to Holmboe, Aug. 3, 1823.

§ Mém. Ac. R. Sc. de l'Institut de France, 6, année 1823, Paris, 1827, pp. 1–60. Reproduced in his Théorie des nombres, ed. 2, second supplément, Sept., 1825, pp. 1–40.

Thus

$$[4]\quad 2x = b^n + c^n - a^n, \qquad 2y = a^n + c^n - b^n, \qquad 2z = a^n + b^n - c^n.$$

Second, let $x$ be divisible by $n$; we obtain results like [3] including

$$[5]\qquad y + z = n^{n-1}A^n, \qquad z + x = b^n, \qquad x + y = c^n.$$

To Sophie Germain is credited the ingenious and important theorem that *if there exists an odd prime p such that*

$$[6]\qquad \xi^n + \eta^n + \zeta^n \equiv 0 \qquad (\mathit{mod}\ p)$$

*has no set of integral solutions* $\xi$, $\eta$, $\zeta$, *each not divisible by p, and if n is not the residue modulo p of the nth power of any integer, then* [1] *has no integral solutions each prime to n.* For, such solutions satisfy also congruence [6], so that one of them, say $x$, is divisible by $p$, whence, by [4],

$$b^n + c^n + (-a)^n \equiv 0 \qquad (\mathrm{mod}\ p).$$

Hence $a$, $b$ or $c$ is divisible by $p$. But, if $b$ were divisible by $p$, then, by [3], $y = -b\beta$ would be divisible by $p$, and hence by [1] also $z$ would be divisible by $p$, whereas $x$, $y$, $z$ have no common factor. Similarly, $c$ is not divisible by $p$. Hence

$$a \equiv 0, \qquad x \equiv 0, \qquad z \equiv -y,$$

$$\phi(x, y) \equiv y^{n-1}, \qquad \phi(y, z) \equiv ny^{n-1} \qquad (\mathrm{mod}\ p).$$

Thus, by [3], $\gamma^n \equiv y^{n-1}$, $\alpha^n \equiv ny^{n-1}$, whence $n\gamma^n \equiv \alpha^n$ (mod $p$). By the final equation [3], $\gamma$ is prime to $p$. Hence we can determine an integer $t$ such that $\gamma t \equiv 1$ (mod $p$). Thus $n \equiv (\alpha t)^n$ (mod $p$), contrary to hypothesis.

The conditions in the theorem are satisfied if $n = 7$, $p = 29$, since the residues of the seventh powers of all integers modulo 29 are $\pm 1$, $\pm 12$, no two of which differ by unity, and since no one of these residues is congruent to 7. Likewise, for each odd prime $n < 100$, S. Germain gave a prime $p$ for which the theorem applies, and hence concluded that Fermat's equation [1] has no integral solutions each prime to $n$, when $2 < n < 100$.

The condition that $n$ shall not be a residue of an $n$th power requires that the prime modulus $p$ be of the form $mn + 1$, where $m$ is even since $p$ is odd. Legendre proved (§§ 23–28) that $m$ must be prime to 3 and that both of the conditions in the theorem hold if $p = mn + 1$ is a prime and $m = 2, 4, 8, 10, 14, 16$, but overlooked the exceptional character of $n = 3$ when $m = 14$ or $16$. He concluded that [1] has no solutions prime to $n$ if $2 < n < 197$.

Legendre proved (§§ 38–47) that $x^5 + y^5 + z^5 = 0$ has no integral solutions. Dirichlet had already presented to the Paris Academy, July 11, 1825, a proof for the case in which $z$ is even, if $z$ is the unknown divisible by 5, and soon published* a proof by a method applying as well to the case $z$ odd, whereas Legendre had treated the two cases by two methods. Dirichlet† proved by the method of descent that [1] is impossible if $n = 14$.

G. Libri‡ proved for $n = 3$ and $n = 4$ and stated for any $n$ that for the primes $p$, exceeding an assignable limit, congruence [6] has solutions prime to $p$, so that it is futile to attempt to prove Fermat's theorem by trying to show that one of the unknowns is divisible by an infinitude of primes.

G. Lamé§ proved Fermat's theorem for the exponent 7. Simplifications were made by V. A. Lebesgue|| and A. Genocchi.¶ The latter** gave the generalization that there is no solution such that $x$, $y$, $z$ are the roots of a cubic equation with rational coefficients. T. Pepin†† gave another proof of Lamé's result and that of Libri for $n = 3$.

In 1883 the Belgian Academy of Sciences offered a prize for a proof of Fermat's last theorem; no award was made.

A. E. Pellet‡‡ found by means of inequalities in the theory of roots of unity that congruence [6], for a prime modulus $p = n\omega + 1$, has solutions each not divisible by $p$ for every $\omega$ exceeding a certain limit (not specified) for which $n\omega + 1$ is a prime. This is the essential part of Libri's assertion quoted above.

E. Wendt§§ noted that, if $n$ and $p = mn + 1$ are odd primes, congruence [6] has no solutions $\xi$, $\eta$, $\zeta$, each prime to $p$, if and only if $p$ is not a divisor of the resultant $D_m$ of

$$[7] \qquad z^m \equiv 1, \qquad (z + 1)^m \equiv 1 \qquad (\text{mod } p).$$

For, if $\omega$ is determined by $\omega\zeta \equiv 1 \pmod{p}$, the product of [6] by $\omega^n$ gives a congruence of the form $z + 1 \equiv y \pmod{p}$, where $z$ and $y$ are $n$th powers,

---

* Jour. für Math., 3, 1828, 354–375; Werke, 1, 1–46.

† Ibid., 9, 1832, 390–3; Werke, 1, 189–194.

‡ Ibid., pp. 270–5.

§ Comptes Rendus, Paris, 9, 1839, 45-6; Mém. prés. divers savants ac. sc. Institut France, 8, 1843, 421–37. Jour. de Math., 5, 1840, 195–211 (pp. 211–5 for report by Cauchy; Oeuvres (1), 4, 499).

|| Jour. de Math., 5, 1840, 276–9, 348–9.

¶ Annali di mat., 6, 1864, 287–8.

** Comptes Rendus, Paris, 78, 1874, 435; 82, 1876, 910-3.

†† Ibid., 82, 1876, 676–9; 91, 1880, 366–8.

‡‡ Bull. Soc. Math. France, 15, 1886–7, 93.

§§ Jour. für Math., 113, 1894, 335–347.

so that their $m$th powers are congruent to unity by Fermat's lesser theorem. Hence S. Germain's theorem may be expressed as follows: If $mn + 1$ is a prime dividing neither $n^m - 1$ nor

$$D_m = \begin{vmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-1} \\ \binom{m}{m-1} & 1 & \binom{m}{1} & \cdots & \binom{m}{m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & 1 \end{vmatrix},$$

Fermat's equation for the prime exponent $n > 2$ is impossible in integers all prime to $n$. The same conclusion follows if $m = 2^\nu n^k$ can be so chosen that $mn + 1$ is a prime not dividing $D_m$, where $\nu$ is not divisible by the prime $n$.

Dickson[*] noted that, if $a$ is a common root of congruences [7],

$$a, \quad \frac{1}{a}, \quad -1-a, \quad \frac{1}{-1-a}, \quad -1-\frac{1}{a}, \quad \frac{-a}{1+a}$$

are common roots and are distinct if $2^m - 1$ is not divisible by $p$. They are the roots of a sextic in $z$ which is unaltered when $z$ is replaced by $1/z$ or by $-1-z$. The sextic must divide $z^m - 1$ modulo $p$. Set $x = z + 1/z$, $m = 2\mu$. The sextic becomes

$$C(x) = x^3 + 3x^2 + \beta x + 2\beta - 5.$$

From $z^\mu - 1/z^\mu = 0$ we get $f(x^2) = 0$, where $f(\omega)$ is of degree $\frac{1}{2}\mu - 1$ or $(\mu - 1)/2$ according as $\mu$ is even or odd. Thus $f(x^2)$ must be divisible by $S(x) = C(x)C(-x) = x^6 + (2\beta - 9)x^4 + (\beta^2 - 12\beta + 30)x^2 - (2\beta - 5)^2$. Hence $\mu \geqq 7$. For $\mu = 7$, $f(x^2) = x^6 - 5x^4 + 6x^2 - 1$ must be congruent to $S(x)$, whence $p = 2$. For $\mu = 8$, $f(x^2) = x^6 - 6x^4 + 10x^2 - 4$, whence $p = 17$, contrary to $n > 1$. The cases $\mu = 10, 11, 13$ are readily treated. The conclusion is that, if $n$ and $p = mn + 1$ are odd primes, $m$ being prime to 3 and $m \leqq 26$, congruence [6] has no integral solutions each prime to $p$, except for $n = 3$, $m = 10, 14, 20, 22, 26$; $n = 5$, $m = 26$; $n = 31$, $m = 22$. A direct examination of [7] was made for $m = 28, 32, 40, 56, 64$. By use of these results and the theorem of S. Germain, it was shown that Fermat's equation is impossible in integers prime to $n$ for every odd prime exponent $n < 1700$.

Dickson[†] proved the last result for $n < 7000$ by extending the range of the $m$'s to include all values $< 74$, as well as 76 and 128.

---

[*] Messenger of Math. (2), 38, 1908, 14–32.

[†] Quart. Jour. Math., 40, 1908, 27–45. The case 6857 was excluded later.

Dickson* proved, by use of Jacobi's functions of roots of unity, that if $n$ and $p$ are odd primes such that

$$p \geqq (n-1)^2(n-2)^2 + 6n - 2,$$

congruence [6] has integral solutions each prime to $p$, thus establishing independently of Pellet the conjecture by Libri in 1832. G. Cornacchia† obtained a like result by the same methods.

It is perhaps superfluous to mention the bequest by P. Wolfskehl to the K. Gesellschaft des Wissenschaften of Göttingen as a prize for a complete proof of Fermat's last theorem.

A. Fleck‡ considered the common factors of the six functions $x^2 + xy + y^2, \cdots, z^2 - xy$ of solutions of Fermat's equation [1].

B. Lind§ gave an account of numerous papers not employing algebraic numbers; of the results claimed as novel, the earlier ones are well known and the later ones erroneous.

A. Pellet|| proved by use of the equation for the $n$ periods of the $p$th roots of unity, where $p = hn + 1$ is a prime, that congruence [6] has solutions not divisible by $p$ if $h^4 > (p-h)^3$, which he stated erroneously to follow from $h > n\sqrt{n}$ [the latter, but not the former, holds if $n = 5$, $h = 20$].

## PART II.

## The Origin of the Theory of Algebraic Numbers

**4. Erroneous views on algebraic numbers prevalent in 1847.** G. Lamé¶ attempted to prove that Fermat's equation for any odd prime exponent $n$ is not satisfied by complex integers

$$[8] \qquad a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

where $\alpha$ is an imaginary $n$th root of unity, and the $a$'s are integers. As pointed out by Liouville (ibid., pp. 315–6), Lamé had not shown that a complex integer is decomposable into complex primes in a single manner. Lamé (p. 352) admitted this lacuna in his proof, but believed (on the basis of extensive tables of factorizations) that it could be filled, affirming (p. 569, p. 888) that the ordinary laws for integers hold for complex integers when $n = 5$. Lamé** presented his arguments in two long memoirs.

---

* Jour. für Math., 135, 1909, 181–8. Cf. Hurwitz, 136, 1909, 272–292.

† Giornale di mat., 47, 1909, 219–268.

‡ Sitzungs. Berliner Math. Gesell., 8, 1909, 133–148; 9, 1910, 50–3.

§ Abh. Geschichte Math. Wiss., 26, II, 1910, 23–65.

|| L'intermédiaire des math., 18, 1911, 81–2.

¶ Comptes Rendus, Paris, 24, 1847, 310–5.

** Jour. de math., 12, 1847, 137–171, 172–184.

E. E. Kummer* pointed out the falsity of Lamé's assumption that every complex integer [8] can be decomposed into primes in a single way. It is an instructive fact that Kummer himself made the same false assumption a short time before in constructing what he then believed to be a complete proof of Fermat's theorem.† The MS. was submitted to Dirichlet, who declared the proof would be as correct as it was elegant if Kummer had proved not merely that every number [8] can be factored into indecomposable numbers, but also that this factorization is possible in only one way, and expressed his belief that unfortunately the numbers [8] do not in general possess this property.

Wantzel‡ proved that Euclid's greatest common divisor process holds for complex integers $a + b\sqrt{-1}$ (as Gauss had shown) and for complex integers $a + b\omega + c\omega^2$ formed from an imaginary cube root $\omega$ of unity, and stated that a like property holds for complex integers [8], with $n$ arbitrary, since the norm of [8] is less than unity when $a_0, \cdots, a_{n-1}$ are between 0 and 1. Here the norm of [8] means the product of [8] by the complex numbers obtained from it by replacing $\alpha$ by the remaining primitive $n$th roots of unity. A. Cauchy§ showed that this statement that the norm is $< 1$ is false for $n = 7$ and for any prime $n = 4m + 1 \geqq 17$, and pointed out lacunæ in Lamé's proof.

Cauchy|| attempted to prove the false theorem that the norm of the remainder obtained on dividing one complex number [8] by another can always be made less than the norm of the divisor. He drew the false conclusion that a product of complex integers [8] can be factored into complex primes in a single manner, and hence that all the laws of divisibility of ordinary integers hold for these complex integers. Next,¶ he assumed that the preceding results hold for a given $n$ and developed at length the conclusions (often false), admitting at the end of the final paper that the basal theorem is false for $n = 23$.

**5. Difficulties presented by an example.** It will tend to concreteness to verify in a simple example the fact, so contrary to the intuitions of the able mathematicians just cited, that the laws of ordinary integers may fail for algebraic integers. As the first case of failure for the algebraic integers [8], determined by an $n$th root of unity, occurs for $n = 23$ and thus presents too much computation to serve as a simple illustration, we shall pass to the simpler example of the set $S$ of all quadratic integers

---

* Comptes Rendus, Paris, 24, 1847, 899; Jour. de math., 12, 1847, 136.

† K. Hensel, Gedächtnisrede auf E. E. Kummer, Abh. Geschichte Math. Wiss., 29, 1910, p. 22.

‡ Comptes Rendus, Paris, 24, 1847, 430–4.

§ Ibid., 469–481; Oeuvres (1), 10, 240–254.

|| Ibid., 516–528; Oeuvres (1), 10, 254–268.

¶ Ibid., 578–84, 633–6, 661–6, 996–9, 1022–30; Oeuvres (1), 10, 268–285, 296–308.

$a + b\theta$, where $\theta = \sqrt{-5}$ and $a$, $b$ are ordinary integers. We have two distinct ways of factoring 9 into indecomposable numbers of the set $S$, viz.,

$$9 = 3 \cdot 3 = (2 + \theta)(2 - \theta). \tag{9}$$

By an indecomposable number $N$ of the set $S$ we mean one having no factor in $S$ other than $N$, $-N$, $+1$, $-1$. Suppose that

$$2 + \theta = (x + y\theta)(z + w\theta),$$

where $x$, $y$, $z$, $w$ are ordinary integers. Then

$$2 - \theta = (x - y\theta)(z - w\theta)$$

and, by multiplication,

$$9 = (x^2 + 5y^2)(z^2 + 5w^2). \tag{10}$$

But $x^2 + 5y^2 = 3$ is evidently not solvable in ordinary integers. Hence one of the factors of the right member of [10] is unity and the other is 9, so that one of the assumed factors of $2 + \theta$ is $\pm 1$. In the same manner, the assumption that 3 is decomposable leads to equation [10], so that one of the two factors is $\pm 1$. Hence the number 9 has the two distinct sets [9] of indecomposable factors in $S$.

Although 3 is indecomposable, it does not have the true character of a quadratic prime, since it divides the final product [9] without dividing either factor $2 \pm \theta$.

Again, there exists no number $\delta$ of $S$ which plays the rôle of a greatest common divisor of 9 and $t = 3 - 6\theta$, so that 9 and $t$ are divisible by $\delta$, while every common divisor of 9 and $t$ is a divisor of $\delta$. In fact, the only factors in $S$ of 9 are 1, 3, 9, $2 \pm \theta$ and their negatives; the only factors of $t$ are 1, 3, $1 - 2\theta$, $2 - \theta$, $4 - \theta$, $t$ and their negatives; so that the only common factors are $\pm 1$, $\pm 3$, $\pm (2 - \theta)$, no one of which is divisible by the remaining five (as shown above).

Hence the laws of arithmetic fail in several respects for the set $S$.

6. **Difficulties removed by use of Kummer's ideal numbers.** It was the fundamental discovery of Kummer* that the set of all complex integers defined by an $n$th root of unity could be so enlarged by the introduction of ideal numbers that unique factorization into primes would prevail in the enlarged set, which would therefore obey the laws of arithmetic as regards multiplication and division. Kummer had in mind immediate applications to Fermat's theorem and the higher reciprocity law.

While Kummer introduced ideal numbers only in the case of complex numbers defined by a root of unity, his method is applicable to the simpler example of § 5, as shown in detail by Dedekind.*

---

* Berichte Ak. Wiss. Berlin, 1845; reprinted in Jour. für Math., 35, 1847, 319, 327. Jour. de math., 12, 1847, 185–212.

The difficulties encountered in § 5 can be overcome by the introduction of ideal prime numbers $\alpha$, $\beta$, $\gamma$, such that

$$[11] \qquad 3 = \alpha\beta, \qquad 2 + \theta = \alpha^2, \qquad 2 - \theta = \beta^2, \qquad 1 - 2\theta = \beta\gamma.$$

Now each member of [9] decomposes further into $\alpha^2\beta^2$, so that there is now only one decomposition of 9 into ideal primes. Moreover, 9 and $3 - 6\theta = \alpha\beta^2\gamma$ now have the greatest common ideal divisor $\alpha\beta^2$.

Kummer did not define the ideal $\alpha$ itself, but gave a general method which when applied to our example affords a definite rule to decide whether or not a quadratic integer $\omega = x + y\theta$ is divisible by $\alpha$, the test for divisibility being that $(1 + \theta)\omega \equiv 0 \pmod{3}$, viz., $x + y \equiv 0 \pmod{3}$. Similarly, $\omega$ is said to have the ideal factor $\beta$ if and only if $(1 - \theta)\omega \equiv 0$, viz., $x - y \equiv 0 \pmod{3}$. Thus $\omega$ has both factors $\alpha$ and $\beta$ if and only if $x \equiv y \equiv 0 \pmod{3}$, i. e., if $\omega$ is divisible by 3, and this accords with our agreement that $\alpha\beta = 3$. In like manner, $\omega$ is said to be divisible by $\alpha^n$ if and only if $(1 + \theta)^n\omega \equiv 0 \pmod{3^n}$; in particular, $\omega$ is divisible by $\alpha^2$ if and only if

$$(1 + \theta)^2\omega = -4x - 10y + (2x - 4y)\theta \equiv 0 \pmod{9},$$

viz., if and only if $x \equiv 2y \pmod{9}$. But the latter is seen to be a necessary and sufficient condition that $\omega$ be divisible by $2 + \theta$ (the quotient being a quadratic integer). Hence in testing for divisors we may identify $\alpha^2$ with $2 + \theta$; and similarly $\beta^2$ with $2 - \theta$, since either is a factor of $\omega$ if and only if $x \equiv -2y \pmod{9}$. Finally, our tests show at once that $1 - 2\theta$ is divisible by $\beta$, but not by $\beta^2$ or $\alpha$.

Having now justified all the formulas [11], we have explained and removed the particular difficulties met in § 5. But the factorization of new numbers of our set $S$ requires the definition of new ideal numbers. An exhaustive investigation would be quite lengthy; moreover, Dedekind has emphasized the delicacy of the subject and the constant need of the greatest circumspection. What precedes may suffice to indicate the point of view of Kummer. It has been completely superceded by the standpoint of Dedekind, which is more concrete, simpler and more general. Not that the fundamental results of Kummer have lost one whit of their importance; a reader of his papers has only to give to his terms the modern interpretation.

**7. Dedekind's ideals.** With Dedekind, an ideal is defined explicitly in terms of the given numbers and hence is more concrete and tangible than the ideal numbers of Kummer, which were not defined themselves but their possible occurrence as factors determined. Moreover, Dedekind's method applies to all algebraic domains and not merely to Kummer's case of domains defined by roots of unity. Accordingly we can select as a medium for our introduction a very simple domain, which shall present the typical difficulties.

---

* Bull. sc. math. astr., 11, 1876, 278; (2), 1, I, 1877, 17, 69, 144, 207.

We shall again consider the set $S$ of all quadratic integers $a + b\theta$, where $\theta = \sqrt{-5}$, and $a$, $b$ are (ordinary) integers. Just as the number 3 determines uniquely all its multiples $3x + 3y\theta$ in $S$, where $x$ and $y$ range over all integers, so any number $\mu$ of $S$ corresponds uniquely to the totality of its multiples in $S$, a totality $\sigma$ called the principal ideal $(\mu)$ and evidently having the following two properties:

*A*. The sum and difference of any two (equal or distinct) numbers of the set $\sigma$ are themselves numbers of the set $\sigma$.

*B*. Every product of a number of the set $\sigma$ by a number of the entire set $S$ is a number of the set $\sigma$.

In other words, the set $\sigma$ is closed under addition and subtraction, as well as under multiplication by numbers of $S$. Any set of numbers of $S$ will be called an ideal if it has these two properties and is not composed exclusively of the number zero.

The principal ideals $(\mu)$ correspond to the numbers $\mu$ of $S$. It will turn out that there exist further ideals and they play the rôle of Kummer's intangible ideal numbers. The principal and other ideals together furnish an enlarged system of elements obeying all the laws of arithmetic relating to divisibility.

8. **Explicit determination of all the ideals.** Since the product of any quadratic integer by its conjugate is an (ordinary) integer, it follows from property $B$ that any ideal $\sigma$ contains integers. Let $k$ be the greatest common divisor of all the integers in $\sigma$, so that $k$ is a linear function of these integers. Then, by property $A$, $k$ occurs in $\sigma$. Likewise, if $m$ is the greatest common divisor of the coefficients of $\theta$ in the various quadratic integers in $\sigma$, then $\sigma$ contains $l + m\theta$, where $l$ is some integer. Thus, by property $A$, $\sigma$ contains the totality $[k, l + m\theta]$ of the linear homogeneous functions of $k$ and $l + m\theta$ with integral coefficients. Moreover, $\sigma$ coincides with that totality. For, let $a + b\theta$ be any number of $\sigma$. If $b = 0$, $a$ is a multiple of $k$. If $b \neq 0$, then $b = qm$, so that $\sigma$ contains

$$a + b\theta - q(l + m\theta) = a - ql,$$

which, being an integer in $\sigma$, is a multiple of $k$.

It remains to require that $\sigma = [k, l + m\theta]$ shall have also property $B$. By the bracket notation, the products of the numbers of $\sigma$ by an integer are in $\sigma$. Hence we may restrict the proof to products of numbers in

$\sigma$ by $\theta$, and thus require that $k\theta$ and $(l + m\theta)\theta = -5m + l\theta$ shall be in $\sigma$. The coefficients $k$ and $l$ must be multiples of $m$. Let $k = ma$, $l = bm$. Then $k\theta = a(l + m\theta) - bk$ is in $\sigma$, while

$$-5m + l\theta = b(l + m\theta) - m(b^2 + 5)$$

is in $\sigma$ if and only if $m(b^2 + 5)$ is divisible by $k$. Hence

$$[12] \qquad \sigma = [ma, m(b + \theta)], \qquad b^2 \equiv -5 \pmod{a},$$

is the desired explicit formula for any ideal. Evidently we may suppress multiples of $a$ from $b$ at will. If $a = 1$, we may therefore set $b = 0$ and obtain $[m, m\theta]$, which is another notation for the principal ideal $(m)$.

9. **Multiplication of ideals.** Recalling that the principal ideal $(\mu)$ is to take the place of the number $\mu$ of $S$, we shall evidently desire that multiplication of ideals shall be such that it will give in particular $(\mu)(\lambda) = (\mu\lambda)$. Accordingly we define multiplication of ideals in general as follows: If $\rho$ ranges over the numbers of an ideal $\sigma$, and $\rho'$ over the numbers of an ideal $\sigma'$, then the products $\rho\rho'$ and their sums and differences form an ideal called the product of $\sigma$ and $\sigma'$, and designated $\sigma\sigma'$.

In particular, the product of [12] by the conjugate ideal

$$\sigma_1 = [ma, m(b - \theta)]$$

is the aggregate of the linear functions with integral coefficients of

$$m^2a^2, \qquad m^2a(b - \theta), \qquad m^2a(b + \theta), \qquad m^2(b^2 + 5).$$

Write $c$ for the integer $(b^2 + 5)/a$. Then

$$\sigma\sigma_1 = [m^2a^2, 2m^2ab, m^2ac, m^2a(b + \theta)].$$

The greatest common divisor of the first three integers is $m^2ag$, if $g$ denotes that of $a$, $2b$, $c$. Since $b^2 + 5 = ac$, $g^2$ divides 20, and $g = 1$ or 2. But if $a$, $c$ were both even, $b^2 + 5 \equiv 0 \pmod{4}$, whereas $b^2 \equiv 0$ or $1 \pmod{4}$. Hence $g = 1$. The greatest common divisor of three numbers equals a linear combination of them. Thus

$$\sigma\sigma_1 = [m^2a, m^2a(b + \theta)] = [m^2a, m^2a\theta] = (m^2a).$$

Hence *the product of any ideal and its conjugate is a principal ideal.*

10. **Division of ideals.** Every number of the product $\rho\sigma$ of two ideals belongs to the ideal $\rho$, as follows at once from the definition of multiplication of ideals and properties $B$ and $A$. Conversely, *if every number of an ideal $\tau$ belongs to an ideal $\rho$, there exists an ideal $\sigma$ such that $\rho\sigma = \tau$,* and $\tau$ is said to be divisible by $\rho$. For, if $\rho_1$ is the conjugate to $\rho$, the numbers of $\tau\rho_1$ belong to the principal ideal $\rho\rho_1 = (r)$, so that the numbers

of $\tau\rho_1$ are $s_1r$, $s_2r$, $\cdots$, where the $s$'s are quadratic integers. Since properties $A$ and $B$ hold for the ideal $\tau\rho_1$, we have

$$s_1r + s_2r = s_ir, \qquad s_1r - s_2r = s_jr, \qquad s(s_1r) = s_kr,$$

for any quadratic integer $s$, where $s_i$, $s_j$, $s_k$ belong to the set $s_1$, $s_2$, $\cdots$. Cancelling the factor $r$, we see that the set of numbers $s_1$, $s_2$, $\cdots$ has the characteristic properties $A$, $B$ of an ideal $\sigma$. Hence $\tau\rho_1 = \sigma(r) = \sigma\rho\rho_1$, whence $\tau = \sigma\rho$. For, an equation $\alpha\beta = \alpha\gamma$ in ideals implies that $\beta = \gamma$. To show this, let $\alpha_1$ be the ideal conjugate to $\alpha$, so that $\alpha\alpha_1$ is a principal ideal $(a)$. Then $\alpha_1\alpha\beta = \alpha_1\alpha\gamma$ or $(a)\beta = (a)\gamma$, and the products of the numbers of $\beta$ by $a$ are identical with the products of the numbers of $\gamma$ by $a$, whence $\beta = \gamma$.

*An ideal $\tau$ is divisible by only a finite number of ideals $\rho$.* For, if $\tau_1$ is the ideal conjugate to $\tau$, $\tau\tau_1$ is a principal ideal $(t)$, where $t$ is an integer. If $\tau = \rho\sigma$, then $(t) = \rho\cdot\sigma\tau_1$, and, by the first remark in this section, $t$ belongs to the ideal $\rho$. But $t$ belongs only to a finite number of ideals $[k, l + m\theta]$, since (§ 8) $k$ is an integer dividing $t$, and $m$ is an integer dividing $k$, while $l$ can be restricted to the values 0, 1, $\cdots$, $k - 1$.

**11. Unique factorization of an ideal into primes.** An ideal, different from the principal ideal (1) and divisible by no ideal other than itself and (1), is called a prime ideal.

*If the prime ideal $\pi$ divides a product $\rho\sigma$, it divides $\rho$ or $\sigma$.* Suppose that $\pi$ does not divide $\rho$. Then the ideal composed of the numbers of both $\pi$ and $\rho$ and their sums and differences contains all the numbers of $\pi$ and hence (§ 10) is a divisor of $\pi$; being distinct from $\pi$, it is (1). Hence $1 = p + r$, where $p$ is some number of $\pi$, and $r$ some number of $\rho$. Let $s$ be any number of $\sigma$. Then $s = ps + rs$. By hypothesis, $rs$ occurs in $\pi$. By property $B$, $ps$ occurs in $\pi$. Hence by property $A$, $s$ occurs in $\pi$. Hence (§ 10), $\sigma$ is divisible by $\pi$.

An ideal not a prime and different from (1) is said to be composite. *Every composite ideal $\sigma$ can be expressed in one and but one way as a product of a finite number of prime ideals.* Since $\sigma$ has a divisor $\sigma_1$, distinct from (1) and $\sigma$, we have $\sigma = \sigma_1\sigma_2$, where $\sigma_2$ is distinct from (1). If one of the ideals $\sigma_1$, $\sigma_2$ is not a prime, it equals a product of two ideals, and we get $\sigma = \sigma_1'\sigma_2'\sigma_3'$. If one of the $\sigma_i'$ is not a prime, it equals a product of two ideals; etc. This process must terminate. For, by the final result of § 10, $\sigma$ is divisible by only a finite number $n$ of ideals, whereas a relation $\sigma = \tau_1\tau_2 \cdots \tau_{n+1}$, in which each ideal $\tau_i$ is distinct from (1), would require that $\sigma$ have the $n + 1$ distinct factors $\tau_1$, $\tau_1\tau_2$, $\cdots$, $\tau_1 \cdots \tau_{n+1}$. Hence our process must lead to a prime ideal factor of $\sigma$. Applying the same result to the quotient, etc., we see that $\sigma$ is a product of a finite number of prime ideals. There cannot be a second such factorization of $\sigma$ into prime ideals in view of the first theorem of this section.

12. **Prime ideals.** Let $p$ be the least positive integer contained in the prime ideal $\pi$. Then $p$ is a prime. For, if $p = rs$, where $r$ and $s$ are integers $> 1$, $\pi$ divides $(p)$ by § 10 and hence also $(r)$ or $(s)$, and $\pi$ would contain the positive integer $r < p$ or $s < p$. Let $\pi$ be given by formula [12]. Then $ma = p$, so that either $m = p$, $a = 1$, or $m = 1$, $a = p$. In the first case, $\pi = [p, p(b + \theta)]$ is the principal ideal $(p)$. In the second case, $\pi = [p, b + \theta]$, where $b^2 \equiv -5 \pmod{p}$, and, if $\pi'$ is the conjugate of $\pi$, $\pi\pi' = (p)$ by § 9. Conversely, if $(p) = \pi\pi'$, $\pi$ is a prime ideal. For, if $\pi = \rho\sigma$, and $\rho\rho' = (r)$, $\sigma\sigma' = (s)$, then $p = rs$ would be composite. Hence *if $p$ is a prime $\neq 2, 5$, $(p)$ is the product of two distinct conjugate prime ideals or is itself a prime ideal according as $-5$ is a quadratic residue or non-residue of $p$; while $(2)$ and $(5)$ are the squares of the prime ideals $[2, 1 + \theta]$ and $[5, \theta]$ respectively. All prime ideals are obtained in this way from the primes $p$.*

13. **Explanation of the difficulties in § 5.** We pass from the quadratic integers $3$, $2 \pm \theta$ to the corresponding principal ideals $(3)$, $(2 \pm \theta)$. By § 12, $(3) = \alpha\beta$, where $\alpha = [3, -1 + \theta]$, $\beta = [3, 1 + \theta]$. Since $(\mu) = [\mu, \mu\theta]$,

$$(2 + \theta) = [2 + \theta, -5 + 2\theta] = [9, 2 + \theta] = \alpha^2 = [9, -3 + 3\theta, -4 - 2\theta].$$

Changing the sign of $\theta$, we see that $(2 - \theta) = \beta^2$. Next,

$$(1 - 2\theta) = [1 - 2\theta, 10 + \theta] = [21, 10 + \theta] = \beta\gamma,$$

where $\gamma = [7, 3 + \theta]$ is one of the prime ideal factors of $(7)$, by § 12. Hence the ideal $(9)$ has the single factorization $\alpha^2\beta^2$ into prime ideals, while $(9)$ and $(3 - 6\theta) = \alpha\beta^2\gamma$ have the greatest common ideal divisor $\alpha\beta^2$. The present explanation of the former difficulties is thus notationally the same as in § 6, but we have now used concrete prime ideals $\alpha$, $\beta$, $\gamma$ in place of Kummer's intangible ideal numbers.

14. **Classes of ideals.** Two ideals $\rho$ and $\sigma$ are called equivalent if there exist principal ideals $(r)$ and $(s)$ such that $\rho(r) = \sigma(s)$. Any two principal ideals are therefore equivalent. If also $\rho$ is equivalent to $\tau$, with $\rho(q) = \tau(t)$, then $\sigma$ is equivalent to $\tau$ since $\sigma(sq) = \rho(rq) = \tau(rt)$. Hence all ideals equivalent to a given one are equivalent to each other and are said to form a class of ideals. The principal class contains all the principal ideals and no others. For, if $\sigma$ is equivalent to $(1)$, $\sigma(s) = (r)$, so that the number $r$ of the product $\sigma(s)$ is in $(s)$, whence $r$ is divisible by $s$, and $\sigma = (r/s)$.

Without resorting to any device, we shall give a direct determination of the classes of ideals for the domain defined by $\theta = \sqrt{-5}$. If $(\alpha)$ is any principal ideal, we may set $\alpha = m(A + B\theta)$, where $A$ and $B$ are relatively prime integers. We can choose integers $r$, $s$ such that

$$\begin{vmatrix} s & -r \\ -A & B \end{vmatrix} = sB - rA = 1.$$

Hence

$$(\alpha) = [\alpha, \alpha\theta] = [s\alpha - r\alpha\theta, -A\alpha + B\alpha\theta] = [m(b + \theta), -ma],$$

$$a = A^2 + 5B^2, \qquad b = sA + 5rB.$$

Thus the principal ideals are given* by [12] in which $a = A^2 + 5B^2$, where $A$ and $B$ are relatively prime. Since 2 is not a value of $a$, the ideal $\rho = [2, 1 + \theta]$ is not a principal ideal. We next find all the ideals $\beta$ equivalent to $\rho$, i. e., for which $\beta(\gamma) = \rho(\delta)$. Let $(\gamma_1)$ be the ideal conjugate to $(\gamma)$, so that $(\gamma)(\gamma_1) = (k)$, where $k$ is an integer. Then $\beta(k) = \rho(\alpha)$, where $\alpha = \delta\gamma_1$. Hence we must examine the product

$$\begin{aligned} \rho(\alpha) &= [2, 1 + \theta][ma, m(b + \theta)] \\ &= [2ma, 2m(b + \theta), ma(1 + \theta), m(b - 5) + m(1 + b)\theta]. \end{aligned}$$

First, let $a$ be odd, $a = 2c + 1$. Since we may add the modulus $a$ to $b$, we may assume that the root $b$ is odd. Since

$$a(1 + \theta) = c(2b + 2\theta) + b + \theta + 2a(1 - b)/2,$$

$$b - 5 + (1 + b)\theta = (1 + b)(b + \theta) - (b^2 + 5),$$

and $b^2 + 5$ is an even multiple of $a$, we have

[13] $$\rho(\alpha) = [2ma, m(b + \theta)], \qquad b^2 \equiv -5 \pmod{2a}.$$

Second, let $a$ be even, $a = 2c$. Since $a$ divides $b^2 + 5$, $b$ is odd, and $b^2 + 5 \equiv 2 \pmod 4$, so that $(b^2 + 5)/a$ is odd. Since

$$a(1 + \theta) = c(2b + 2\theta) + 2a(1 - b)/2,$$

$$b - 5 + (1 + b)\theta = \tfrac{1}{2}(b + 1)(2b + 2\theta) - (b^2 + 5),$$

we have

[14] $$\rho(\alpha) = [2m \cdot a/2, 2m(b + \theta)], \qquad b^2 \equiv -5 \pmod{a/2}.$$

Thus the ideals $\beta$ equivalent to $\rho$ are those for which $\beta(k)$ is of the form [13] or [14], where $k$ is an integer dividing $m$ or $2m$ respectively. But $m$ ranges over all integers. Hence the ideals equivalent to $\rho$ are given by [13] and [14], with $m$ and $2m$ replaced by an arbitrary integer $M$, while $a$ is any integer of the form $A^2 + 5B^2$, with $A$ and $B$ relatively prime. For $a$ odd, $1 \equiv A - B \pmod 2$ and

---

* As a check, note that $b^2 + 5 = b^2 + 5(sB - rA)^2 = a(s^2 + 5r^2)$.

$$2a = 2x^2 + 2xy + 3y^2, \qquad x = A - B, \qquad y = 2B,$$

so that $x$ and $y$ are relatively prime. For $a$ even, $A \equiv B \equiv 1 \pmod 2$ and

$$\frac{a}{2} = 2x^2 + 2xy + 3y^2, \qquad x = \frac{A - B}{2}, \qquad y = B,$$

so that $x$ and $y$ are relatively prime integers. Combining the two cases, we conclude that all the ideals equivalent to $\rho = [2, 1 + \theta]$ are

$$[15] \quad [MN, M(b + \theta)], \qquad b^2 \equiv -5 \pmod N, \qquad N = 2x^2 + 2xy + 3y^2,$$

where $x$, $y$ are relatively prime integers.

The class $C$ of the principal ideals and the class $C'$ of the ideals [15] together give all the ideals [12]. For, if $a$ has any value admissible in [12], not merely the preceding special value, there exists an integer $l$ such that $b^2 = -5 + al$ and the form $ax^2 + 2bxy + ly^2$ is of determinant $-5$ and hence* can be transformed into $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ by a linear transformation with integral coefficients of determinant unity. Our general form reduces to $a$ for $x = 1$, $y = 0$. Hence $a$ can be represented by one of our two special forms by means of relatively prime integers $x$, $y$. If it be the first form, the ideal [12] has been shown to be a principal ideal; if it be the second form, the ideal is of type [15] and is equivalent to $[2, 1 + \theta]$.

All the ideals have been distributed into two classes $C$ and $C'$ and an explicit formula has been given for the ideals in each class. The two classes can be distinguished very simply as follows. For an ideal [12] in $C$, $a \equiv x^2 \pmod 5$, so that $a$ is a quadratic residue of 5. For an ideal [15],

$$2N = (2x + y)^2 + 5y^2,$$

so that $2N$ is a residue and $N$ is a non-residue of 5 if $N$ be prime to 5.

The above method of proving that there are only two classes of ideals in the domain employed has not only the advantage of being elementary and exhibiting explicitly all the ideals in each class, but also of illustrating the essential† identity of the problems to find the number of classes of ideals in a quadratic domain of discriminant $d$ and the number of classes of binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = d$.

---

* The two forms are the only reduced forms, i. e., having $l \geqq a \geqq 2|b|$.

† In the present case, every number has a positive norm. But in general, we must employ narrowly equivalent ideals (Dirichlet-Dedekind, Zahlentheorie, p. 578, p. 584) whose ratio is a number of positive norm. To every narrow class of ideals in a quadratic field of discriminant $d$ corresponds one and but one class of quadratic forms of discriminant $d$ capable of representing positive numbers.

**15. Another method for the preceding problem.** The usual method of finding the number of classes of ideals in our domain $F(\sqrt{-5})$ of discriminant $-5\cdot 4$ is based upon the fact that every ideal [12] contains a number $\alpha = r + s\theta \neq 0$ whose norm $r^2 + 5s^2$ does not exceed $m^2 a\sqrt{20}$. We may take

$$\alpha = xma + ym(b + \theta), \qquad r = m(ax + by), \qquad s = my.$$

By the well-known theorem due to Minkowski,* we can choose rational integers $x$, $y$ not both zero such that

$$| ax + by | \leqq \sqrt{a\sqrt{5}}, \qquad | y | \leqq \sqrt{a/\sqrt{5}},$$

since the determinant $a$ of the linear functions equals the product of the two radicals. Hence, as desired,

$$(ax + by)^2 + 5y^2 \leqq a\sqrt{20}.$$

Consider an ideal $A$ of any class $K$ of ideals. Call $B$ the ideal [12] which is conjugate to $A$, so that $BA$ is a principal ideal $(q)$, by § 9. As just proved, $B$ contains a number $\alpha$ of norm $\leqq m^2 a\sqrt{20}$. Then (§ 10), $(\alpha)$ is divisible by $B$; let $Q$ be the quotient. The norm of [12] is $m^2 a$ by definition. It is easily verified that the product of the norms of $B$ and $Q$ equals the norm of their product $(\alpha)$. Thus [norm $Q$] $\leqq \sqrt{20}$. From $BQ = (\alpha)$, $BA = (q)$ follows $A(\alpha) = Q(q)$, so that $A$ and $Q$ are equivalent ideals. Hence any class $K$ contains an ideal of norm $\leqq \sqrt{20}$, and hence an ideal [12] whose norm $m^2 a$ equals 1, 2, 3 or 4. If $a = 1$, the ideal is a principal ideal (§ 10). If $a > 1$, $m = 1$, while $a = 4$ is excluded since $b^2 \equiv -5 \pmod{4}$ is not solvable. If $a = 2$, we have $b = 1$ and the ideal is $[2, 1 + \theta] = \rho$. If $a = 3$, we have $b = \pm 1$ and the ideals are $[3, 1 + \theta] = \beta$ and $[3, -1 + \theta] = \beta'$. Then $\beta\beta' = (3)$ and

$$\rho\beta' = [6, -2 + 2\theta, 3 + 3\theta] = [6, \theta - 1] = (\theta - 1).$$

Multiply this by $\beta$. Hence $\rho(3) = \beta(\theta - 1)$, so that $\rho$ and $\beta$ are equivalent. Changing the sign of $\theta$ throughout, we see that $\rho$ and $\beta'$ are equivalent. Hence the principal class and the class containing $\rho$ are the only classes.

**16. Kummer's class number $H$.** For the domain defined by an imaginary $\lambda$th root $\alpha$ of unity, where $\lambda$ is an odd prime, Kummer† proved that the number of classes of ideals is the product $H = h_1 h_2$ of the two integers

---

* Cf. Hurwitz, Göttingen Nachrichten, 1897; J. Sommer, Vorlesungen über Zahlentheorie, 1907, p. 71.

† Bericht Akad. Wiss. Berlin, 1847, 305–319. Jour. für Math., 40, 1850, 93–129. Jour. de math., 16, 1851, 454–498.

$$h_1 = \frac{P}{(2\lambda)^{\mu-1}}, \qquad h_2 = \frac{D}{\Delta},$$

where $\mu = (\lambda - 1)/2$, and $P$, $D$, $\Delta$ are defined as follows. Let $\beta$ be a primitive root of $\beta^{\lambda-1} = 1$ and $g$ a primitive root of $\lambda$. Then

$$P = \prod_{j=1}^{\mu} \phi(\beta^{2j-1}), \qquad \phi(\beta) = 1 + g_1\beta + g_2\beta^2 + \cdots + g_{\lambda-2}\beta^{\lambda-2},$$

where $g_i$ is the least positive residue of $g^i$ modulo $\lambda$. Next,

$$e(\alpha) = \sqrt{\frac{(1-\alpha^g)(1-\alpha^{-g})}{(1-\alpha)(1-\alpha^{-1})}}$$

is a complex unit (a divisor of 1). Then, if $lx$ denotes $\log x$,

$$D = \begin{vmatrix} le(\alpha) & le(\alpha^g) & \cdots & le(\alpha^{g^{\mu-2}}) \\ le(\alpha^g) & le(\alpha^{g^2}) & \cdots & le(\alpha^{g^{\mu-1}}) \\ \cdot & \cdot & \cdot & \cdot \\ le(\alpha^{g^{\mu-2}}) & le(\alpha^{g^{\mu-1}}) & \cdots & le(\alpha^{g^{2\mu-4}}) \end{vmatrix}.$$

Let $\epsilon_1(\alpha), \cdots, \epsilon_{\mu-1}(\alpha)$ be units such that products of powers of them multiplied by $\pm\,\alpha^m$ give all the units. Then

$$\Delta = \begin{vmatrix} l\epsilon_1(\alpha) & \cdots & l\epsilon_{\mu-1}(\alpha) \\ \cdot & \cdot & \cdot \\ l\epsilon_1(\alpha^{g^{\mu-2}}) & \cdots & l\epsilon_{\mu-1}(\alpha^{g^{\mu-2}}) \end{vmatrix}.$$

It is shown that $h_1$ is divisible by $\lambda$ if and only if $\lambda$ divides the numerator of one of the first $(\lambda - 3)/2$ Bernoullian numbers $B_1 = 1/6$, $B_2 = 1/30, \cdots$; while if $h_2$ is divisible by $\lambda$ also $h_1$ is, but not conversely.

## PART III.

### Application of Algebraic Numbers to Fermat's Last Theorem.

17. Kummer[*] proved that $x^\lambda + y^\lambda = z^\lambda$ is impossible in integers if $\lambda$ is an odd prime not dividing $H$ (§ 16) and hence not the numerator of any one of the first $(\lambda - 3)/2$ Bernoullian numbers. To indicate the nature of the proof for the case in which $x$, $y$, $z$ are prime to $\lambda$, denote the factor $z - \alpha^j y$ of $z^\lambda - y^\lambda$ by $f_j$. The greatest common ideal divisor $G$

---

[*] Bericht Akad. Wiss. Berlin, 1847, 132–9. The proof has been given in modern form, by use of Dedekind's ideals, by D. Hilbert, Jahresbericht Deutschen Math.-Vereinigung, 4, 1894–5, 517–25. Cf. E. Schönbaum, Casopis, 37, 1908, 384–506 (Bohemian).

of any two $(f_j)$ is that of $(z)$ and $(y)$. The product of the $(f_j)$ is $(x)^\lambda$. Hence $(f_j) = GJ_j^\lambda$, where no two $J$'s have a common factor. Thus $J_j^\lambda$ and $J^\lambda_{\lambda-1}$ are equivalent ideals. But the $H$th power of any ideal is a principal ideal, so that $J_j^H$ and $J^H_{\lambda-1}$ are equivalent. Since $\lambda$ does not divide $H$, it follows that $J_j$ and $J_{\lambda-1}$ are equivalent. Thus $(f_j)$ and $(f_{\lambda-1})$ are proportional to the $\lambda$th powers of two principal ideals. It follows readily that

$$f_j = \alpha^{e_j} u_j \tau_j^\lambda \qquad (j = 0, 1, \cdots, \lambda - 2),$$

where $u_j$ is a real unit and $\tau_j$ a number of our domain $F(\alpha)$. A discussion of these equations between ordinary complex numbers leads to a contradiction.

Cauchy* stated that $a^n + b^n + c^n = 0$ is impossible in relatively prime integers not divisible by the odd prime $n$ if

$$1 + 2^{n-4} + 3^{n-4} + \cdots + \left(\frac{n-1}{2}\right)^{n-4}$$

is not divisible by $n$ [i. e., if $B_k$ is not divisible by $n$ for $k = (n - 3)/2$].

Kummer† proved that Fermat's equation for an odd prime exponent not dividing $H$ has no solution in complex integers $a_0 + a_1\alpha + a_2\alpha^2 + \cdots$, where $\alpha^\lambda = 1$. Thus there is no solution for $\lambda < 100$, except perhaps for $\lambda = 37, 59, 67$.

The French Academy of Sciences‡ had offered a gold medal of value 3000 francs for a complete proof of Fermat's last theorem. The prize was awarded to Kummer in 1857 for his investigations on complex integers, although he had not been a competitor.

Kummer§ proved that for any relatively prime integral solutions of $x^\lambda + y^\lambda = z^\lambda$, where $\lambda$ is an odd prime,

$$[16] \qquad B_{(\lambda-i)/2} P_i(x, y) \equiv 0 \pmod{\lambda} \qquad (i = 3, 5, \cdots, \lambda - 2),$$

where $B_j$ is the $j$th Bernoullian number and $P_i(x, y)$ is the homogeneous polynomial of degree $i$ for which

$$\left(\frac{d^i \log(x + e^v y)}{dv^i}\right)_{v=0} = \frac{P_i(x, y)}{(x + y)^i}.$$

He proved that Fermat's equation is impossible in integers for odd prime exponents $\lambda$ which satisfy the following three conditions. (i) The factor $h_1$ of the class number $H$ is divisible by $\lambda$, but not by $\lambda^2$. (ii) For

---

* Comptes Rendus, Paris, 25, 1847, 181; Oeuvres (1), 10, 364. Genocchi, Jour. für Math., 99, 1886, 316.

† Jour. für Math., 40, 1850, 130–8; Jour. de Math., 16, 1851, 488–98.

‡ Comptes Rendus, 29, 1849, 23; 30, 1850, 263–4; 44, 1857, 158.

§ Abhand. Ak. Wiss. Berlin, 1857, Math., 41–74.

$e(\alpha)$, $g$ and $\mu$ defined in § 16, and for the integer $\nu < (\lambda - 1)/2$ such that $B_\nu \equiv 0 \pmod{\lambda}$, there exists an ideal with respect to which as a modulus the unit

$$E_\nu(\alpha) = \prod_{k=0}^{\mu-1} e(\alpha^{g^k})^{g^{-2k\nu}}$$

is not congruent to a $\lambda$th power, whence the second factor $h_2$ of $H$ is not divisible by $\lambda$. (iii) The Bernoullian number $B_{\nu\lambda}$ is not divisible by $\lambda^3$. All three conditions are satisfied when $\lambda = 37, 59, 67$, the values $< 100$ of $\lambda$ for which he had not previously proved Fermat's theorem.

D. Mirimanoff* proved Fermat's theorem for the exponent 37 by use of ideals.

E. Maillet† proved that Fermat's equation with the exponent $\lambda^t$ is impossible in complex integers, prime to $\lambda$, formed from a $\lambda$th root of unity, if $\lambda$ is a prime $> 3$ and $\lambda^{t-1}$ is the highest power of $\lambda$ dividing the class number $H$.

Maillet‡ found by Kummer's method a variety of general values of $c$ for which $x^\lambda + y^\lambda = cz^\lambda$ is impossible when $\lambda$ is a regular prime (i. e., not a divisor of $H$); also§ when $c$ equals $\lambda$ or specified multiples of $\lambda$, for various $\lambda$'s.

Mirimanoff|| considered

$$x^\lambda + y^\lambda + z^\lambda = 0 \qquad [17]$$

for the case in which no one of the integral solutions $x, y, z$ is divisible by the odd prime $\lambda$. By use of Kummer's congruences [16], he proved that [17] is impossible in integers prime to $\lambda$ if at least one of the Bernoullian numbers¶ $B_{\nu-1}, B_{\nu-2}, B_{\nu-3}, B_{\nu-4}$ is not divisible by $\lambda$, where

$$\nu = (\lambda - 1)/2;$$

also, for every $\lambda < 257$. In terms of Kummer's $P_i(t) = P_i(1, t)$, he defined the polynomials

$$\phi_i(t) = (1 + t)^{\lambda - i} P_i(t) \equiv \sum_{k=1}^{\lambda-1} (-1)^{k-1} k^{i-1} t^k \quad (i = 2, 3, \cdots, \lambda - 1) \qquad [18]$$

modulo $\lambda$. Thus Kummer's criterion [16] is equivalent to the following. If [17] has solutions prime to $\lambda$, each of the six ratios $t = x/y, \cdots, z/x$

---

* Jour. für Math., 111, 1893, 26–30.

† Assoc. franc. avanc. sc., 26, 1897, II, 156–168.

‡ Acta Mathematica, 24, 1901, 247–256.

§ Annali di mat. (3), 12, 1905, 145–178.

|| Jour. für Math., 128, 1905, 45–68.

¶ If $B_{\nu-1}$ or $B_{\nu-2}$ is not divisible by $\lambda$, the conclusion was drawn by Kummer in his 1857 paper.

satisfies the congruences

[19] $$B_{(\lambda-i)/2}\,\phi_i(t) \equiv 0 \pmod{\lambda} \qquad (i = 3, 5, \cdots, \lambda - 2).$$

An equivalent criterion not involving Bernoullian numbers is that each of the six ratios satisfies the congruences

[20] $$\phi_{\lambda-1}(t) \equiv 0, \qquad \phi_{\lambda-i}(t)\phi_i(t) \equiv 0 \pmod{\lambda} \qquad (i = 2, 3, \cdots, \nu).$$

A. Wieferich* proved by means of [19] that, if Fermat's equation has solutions each prime to the exponent $p$, then

[21] $$2^{p-1} \equiv 1 \pmod{p^2}.$$

The $k$th derivative with respect to $v$ of

$$te^v - t^p e^{pv} = (1 + te^v)\sum_{i=1}^{p-1}(-1)^{i-1}t^i e^{iv}$$

gives for $v = 0$, on writing $\theta$ for $(1 + t)/t$,

$$\theta\phi_{k+1} + \binom{k}{1}\phi_k + \binom{k}{2}\phi_{k-1} + \cdots + \binom{k}{k}\phi_1 = 1 - t^{p-1}p^k.$$

Taking $k = 0, 1, \cdots$ and solving these linear equations, we get

$$\phi_{k+1} \equiv \frac{(-1)^{k-1}k!\,F_k}{\theta^k} \pmod{p}, \qquad F_i = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{i-1} & \alpha_i \\ \theta & \alpha_1 & \cdots & \alpha_{i-2} & \alpha_{i-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \theta & \alpha_1 \end{vmatrix},$$

where $\alpha_i = 1/i!$. Let $G_i$ be the determinant derived from $F_i$ by replacing $\alpha_j$ in the $r$th row by $\binom{k-r+1}{j}$ for $r = 1, \cdots, i$: Thus $(k - i)!\,G_i = k!\,F_i$. By evaluating $G_k$, we find that

$$-\theta\phi_{k+1} \equiv -H_{k+1} + \theta\lambda^k + \binom{k}{1}H_k\phi_2 + \cdots + \binom{k}{k-1}H_2\phi_k \pmod{p},$$

where $H_{i+1} = (1 + \lambda)^i - (\theta - 1)\lambda^i$, $\lambda$ being arbitrary. Summing for $\lambda = 0, -1, 2, -3, \cdots, p - 1, -p$ and setting $\mathfrak{B}_{2j} = \Sigma(-\lambda)^{2j-1}$ and replacing $k$ by $2k - 1$, we get

[22] $$-\theta\phi_{2k} \equiv -2\mathfrak{B}_{2k} + (2 - \theta)\left\{\binom{2k-1}{2}\mathfrak{B}_{2k-2}\phi_3 + \cdots + \binom{2k-1}{2k-2}\mathfrak{B}_2\phi_{2k-1}\right\} \pmod{p}.$$

If $B_j$ is the $j$th Bernoullian number, it is known that

$$\mathfrak{B}_{2j} \equiv (-1)^{j-1}B_j(2^{2j} - 1)/j \pmod{p}.$$

---

* Jour. für Math., 136, 1909, 293–302.

Hence, taking $k = (p - 1)/2$ and applying [19], we get

$$2\mathfrak{B}_{p-1} \equiv \theta\phi_{p-1} \equiv \frac{\theta}{p}\{(1 + t)^p - 1 - t^p\} \equiv 0 \pmod{p},$$

since $t$ is the ratio of two values satisfying [17]. But $\mathfrak{B}_{p-1} \equiv (2^p - 2)/p$.

D. Mirimanoff* employed Euler's expression for $1 - 2^{p-2} + 3^{p-2} - \cdots \pm y^{p-2}$ as a polynomial in $y$, took $y = 1, 2, \cdots, p - 1$, multiplied the resulting equations by $t, t^2, \cdots, t^{p-1}$, added, multiplied the sum by $t - 1$, and obtained

$$[1^{p-2} - 2^{p-2} + \cdots - (p - 1)^{p-2}]t^p - \tfrac{1}{2}(t + 1)\phi_{p-1}$$
$$= (t - 1)\sum_{j=1}^{\nu-1}(-1)^{j-1}\binom{p - 2}{2j - 1}\frac{2^{2j} - 1}{2j}B_j\phi_{p-2j} + (-1)^{\nu-1}\frac{2^p - 2}{p - 1}B_\nu\frac{t^p - 1}{t + 1},$$

where $\nu = (p - 1)/2$ and $\phi_i$ is given by [18]. The final term is a multiple of $p$ for every $t$; dropping it, we get [22] for $k = (p - 1)/2$. Or, we may apply [19] and [$20_1$] and conclude that

$$0 \equiv 1^{p-2} - 2^{p-2} + \cdots - (p - 1)^{p-2} \equiv (2^p - 2)/p \pmod{p}.$$

G. Frobenius† deduced [21] from [19] and [$20_1$] by showing that

$$\sum_{r, s=0}^{\lambda-1}(-1)^{r-s}(r - s)^{\lambda-2}t^s$$

is congruent modulo $\lambda$, for every $t \not\equiv 0, \pm 1$, to both

$$c = \phi_{p-1}(1), \qquad \frac{1 + t}{1 - t}c,$$

whence $c \equiv 0 \pmod{\lambda}$, which gives [21].

E. Hecke‡ proved that [17] is impossible in integers $x, y, z$ each not divisible by the odd prime exponent $\lambda$ such that the factor $h_1$ of $H$ is divisible by $\lambda$, but not by $\lambda^2$.

D. Mirimanoff§ proved that if there are solutions of

$$x^p + y^p + z^p = 0$$

prime to $p$, each of the six ratios $x/y, \cdots$ is a root $t$ of

$$[23] \quad \prod_{i=1}^{m-1}(t + \alpha_i)\sum_{i=1}^{m-1}\frac{R_i}{t + \alpha_i} \equiv 0 \pmod{p}, \qquad R_i = \frac{\phi_{p-1}(-\alpha_i)}{(1 - \alpha_i)^{p-1}},$$

---

* L'enseignement math., 11, 1909, 455-9.

† Sitzungs. Ak. Wiss. Berlin, 1909, 1222-4; Jour. für Math., 137, 1910, p. 314-6.

‡ Göttingen Nachrichten, 1910, 420-4.

§ Comptes Rendus, Paris, 150, 1910, 204-6. See his paper of 1911.

where $\alpha_1, \cdots, \alpha_{m-1}$ are the roots $\neq 1$ of $z^m = 1$; also,

$$q(m) = \frac{m^{p-1}-1}{p} \equiv \sum_{i=1}^{m-1} \frac{R_i}{1-\alpha_i} \pmod{p}.$$

For $m = 2$ or 3, the degree of [23] is $< 2$, whereas at least two of the six ratios are incongruent; thus [23] is an identity. Taking $t = -1$, we get $q(m) \equiv 0$. In addition to Wieferich's criterion $q(2) \equiv 0$, we have $q(3) \equiv 0$.

G. Frobenius* proved the last two criteria and deduced [19] from [16] more simply than had Mirimanoff. With Lucas,† set $b^{2n} = (-1)^{n-1}B_n$, $b^{2n+1} = 0$, $b^1 = -\frac{1}{2}$, so that the Bernoullian numbers are given by $(b+1)^n - b^n = 0$ if $n > 1$. Set

$$F(x, y) = \sum_{r=0}^{p-1} \binom{y}{r} (x-1)^r,$$

$$F(x, y)x^m = \sum_r \binom{y+m}{r} (x-1)^r + (x-1)^p G(x, y),$$

$$mxG_m(x) = G(x, mb) - G(0, mb)\frac{x^m-1}{x-1},$$

$$mF(x) = F(x, mb) - \{F(0, mb) - mpq\}(x-1)^{p-1}.$$

Then

$$F(x)(x^m-1) + \sum_{n=1}^{p-1} \frac{1-x^n}{n} = (x-1)^p x G_m(x),$$

from which the results of the paper follow. The six ratios of the three solutions prime to $p$ of Fermat's equation satisfy the congruence $G_m(x) \equiv 0 \pmod{p}$ of degree $m-2$. Hence, if $m = 2$ or 3, $G_m$ vanishes identically. But $G_m(1) \equiv (1 - m^{p-1})/p$.

F. Bernstein‡ proved Fermat's theorem under assumptions milder than those used by Kummer in 1857. For the case in which one of the numbers $x, y, z$ is divisible by the prime exponent $\lambda$, it suffices to assume that the number of classes of ideals for the field $k(Z)$ of the $\lambda^2$th roots of unity is divisible by $\lambda$, but not by $\lambda^2$; or, to assume that $k(Z)$ contains no class belonging to the exponent $\lambda^2$, while the number of classes for $k(\alpha + \alpha^{-1})$, where $\alpha^\lambda = 1$, is prime to $\lambda$. For the case in which $x, y, z$ are prime to $\lambda$, it suffices to assume (i) the factor $h_2$ of the number $H$ of classes in $k(\alpha)$ is divisible by $\lambda$, and (ii) if $\lambda^\mu$ is the highest power of $\lambda$ dividing $h_2$, then in the Teilklassenkörper of the $\lambda^\mu$th degree every ideal of $k(\alpha)$, whose $\lambda$th power is a principal ideal in $k(\alpha)$, is itself a principal ideal.

---

* Sitzungs. Ak. Wiss. Berlin, 1910, 200–8.

† Earlier in Blissard, Quar. Jour. Math., 1861, 279.

‡ Göttingen Nachrichten, 1910, 482–8, 507–16.

Ph. Furtwängler* proved, in extension of Kummer's work, that if $\alpha^l + \beta^l + \gamma^l = 0$, where $\alpha$, $\beta$, $\gamma$ are numbers, prime to $L = (\zeta - 1)$, of the field $k(\zeta)$, $\zeta^l = 1$, and if $\alpha \equiv a$, $\beta \equiv b$, $\gamma \equiv c \pmod{L}$, where $a$, $b$, $c$ are rational, and if $k(\zeta)$ contains no ideal belonging† to the exponent $2j + 1$ modulo $L$, then, if $x$, $y$ are any two of $a$, $b$, $c$,

$$\left[\frac{d^{2j+1}\log(x + e^v y)}{dv^{2j+1}}\right]_{v=0} \equiv 0 \pmod{l}.$$

By Mirimanoff's paper of 1905, this congruence can not hold when $j = 1, 2, 3$ or 4. Hence if $k(\zeta)$ does not contain ideals belonging to each of the exponents 3, 5, 7, 11, Fermat's equation is impossible in numbers prime to $l$ in $k(\zeta)$. The same conclusion holds if the class number $H$ is at most divisible by $l^3$.

Mirimanoff‡ reproduced his paper of 1910 and used his formula [23] to obtain results concerning $q(5)$ and $q(7)$. He proved that $\phi_{p-1}(t)$ is divisible by $p$ not only when $t$ is one of the six ratios $\tau = x/y, \cdots$, but also for $t = -\tau$ and $t = -\tau^2$. Finally, he proved Sylvester's§ formula

$$q(m) \equiv \sum_{n=1}^{p-1} \frac{x_n}{p-n} \pmod{p}, \qquad x_n \equiv \frac{n}{p} \pmod{m}.$$

Ph. Furtwängler|| proved by use of Eisenstein's law of reciprocity for residues of $l$th powers, where $l$ is an odd prime, that every integral divisor $r$ of $x_i$ satisfies

$$r^{l-1} \equiv 1 \pmod{l^2} \tag{24}$$

if $x_1$, $x_2$, $x_3$ are relatively prime solutions $\neq 0$ of $x_1^l + x_2^l + x_3^l = 0$ and $x_i$ is prime to $l$. Since one of the $x$'s is divisible by 2, we have the criterion [21] of Wieferich. Next, every factor $r$ of $x_i \pm x_k$ satisfies [24] if $x_i + x_k$ and $x_i - x_k$ are prime to $l$. Since one of the $x$'s is divisible by 3 unless all three are congruent modulo 3, it follows from the two theorems that, if the $x$'s are all prime to $l$, [24] holds for $r = 3$, which is the criterion of Mirimanoff.

S. Bohnicek¶ proved that integral numbers of the domain of the $2^n$th roots of unity do not satisfy Fermat's equation with the exponent $2^{n-1}$, $n > 2$.

---

* Ibid., 554–562.

† An ideal $Q$, prime to $L = (\zeta - 1)$, is said to belong to the exponent $n$ modulo $L$ if $Q^l$ is a principal ideal $(\kappa)$ such that $\kappa \equiv r_1 \pmod{L^n}$, while there exists no unit $\eta$ in the field $k(\zeta)$ such that $\eta\kappa \equiv r_2 \pmod{L^{n+1}}$, where $r_1$ and $r_2$ are rational numbers.

‡ Jour. für Math., 139, 1911, 309–324.

§ Comptes Rendus, Paris, 52, 1861, 161, 212, 307, 817; Phil. Mag., 21, 1861, 136. Math. Papers, II, 229–235, 241, 262–3. Errors in early enunciations.

|| Sitzungs. Ak. Wiss. Wien (Math.), 121, 1912, IIa, 589–592.

¶ Ibid., 727–742

H. S. Vandiver* applied the preceding theorems by Furtwängler and [23] to show that if Fermat's equation has integral solutions each prime to the exponent $p$ and if $q(2) \not\equiv 0 \pmod{p^3}$, then $q(5) \equiv 0 \pmod{p}$ for $p \equiv 1 \pmod{3}$, and $q(5) \equiv q(7) \equiv 0 \pmod{p}$ for $p \equiv 2 \pmod{3}$.

Vandiver† applied [19], [$20_1$] and [23] to show that if Fermat's equation has integral solutions each prime to the exponent $p$,

$$q(5) \equiv 0, \qquad 1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \frac{1}{[p/5]} \equiv 0 \pmod{p}.$$

G. Frobenius‡ proved that if Fermat's equation has integral solutions each prime to the exponent $p$ then $q(m)$ is divisible by $p$ for $m = 11$ and $m = 17$ and, in case $p \equiv 5 \pmod{6}$, also for $m = 7, 13, 19$. Moreover,

$$\sum_{l=1}^{m-1} \left\{ \frac{(l/m + h)^{p-1} - h^{p-1}}{p-1} \right\} x^l$$

vanishes identically modulo $p$ for $m \leqq 22$ and $m = 24, 26$. Here the symbolic power $h^\lambda$ is to be replaced by the Bernoullian number $b_\lambda$.

**18. Further papers on the function $q(m)$.** Eisenstein§ noted that

$$q(uv) \equiv q(u) + q(v), \qquad q(u + pv) \equiv q(u) - \frac{v}{u} \pmod{p},$$

$$2q(2) \equiv 1 - \tfrac{1}{2} + \tfrac{1}{3} - \cdots - \frac{1}{p-1} \equiv \frac{1}{(p-1)/2} + \cdots + \frac{1}{p-1} \pmod{p}.$$

J. Plana|| set $S_i = 1^i + \cdots + (m-1)^i$ and proved that

$$m^j - m = jS_{j-1} + \binom{j}{2} S_{j-2} + \binom{j}{3} S_{j-3} + \cdots + jS_1.$$

M. A. Stern¶ set also $\sigma_i = 1^i + \cdots + m^i$ and proved that

$$\begin{aligned} \frac{m^p - m}{p} &\equiv S_1 - \tfrac{1}{2}S_2 + \cdots - \frac{1}{p-1} S_{p-1} \\ &\equiv \sigma_{p-1} + \tfrac{1}{2}\sigma_{p-2} + \cdots + \frac{1}{p-1}\sigma_1 \\ &\equiv \tfrac{1}{2}\left( \frac{m}{p-1} + \frac{m^2}{p-2} + \cdots + m^{p-1} \right) \\ &\qquad + \frac{1}{p-2} S_2 + \frac{1}{p-4} S_4 + \cdots + S_{p-1}, \end{aligned}$$

---

* Trans. Amer. Math. Soc., 15, 1914, 202–4.

† Jour. für Math., 144, 1914, 314–8.

‡ Sitzungs. Ak. Wiss. Berlin, 1914, 653–681.

§ Berlin Bericht, 1850, 41.

|| Mem. Acad. Turin (2), 20, 1863, 120.

¶ Jour. für Math., 100, 1887, 182–8.

modulo $p$. Mirimanoff* proved the corrected form of Sylvester's formula. This was done also by J. W. L. Glaisher,† who‡ obtained other expressions for $q(m)$.

Lerch § treated at length $q(m)$ and $(a^{\phi(N)} - 1)/N$ for $N$ composite. H. F. Baker|| gave a formula for the latter quotient which generalizes Sylvester's. Friedmann and Tamarkine¶ gave formulas connecting $q(m)$ with Bernoullian numbers and with the greatest integer in $m/p$.

A. Cunningham** verified that $2^p - 2$ is not divisible by $p^2$ for any prime $p < 1000$, nor $3^p - 3$ by $p^2$ for a prime $p = 2^a \cdot 3^b + 1 < 100$.

W. Meissner†† gave the least residue of $(2^t - 1)/p$ modulo $p$ for each prime $p < 2000$, where $t$ is the exponent to which 2 belongs. The only case in which $2^p - 2$ is divisible by $p^2$ for $p < 2000$ is when $p = 1093$.

P. Bachmann‡‡ obtained expressions for $q(m)$.

H. S. Vandiver¶¶ proved that $q(2) \equiv 0 \pmod{p^2}$ if and only if

$$1 + \tfrac{1}{3} + \cdots + \frac{1}{p-2} \equiv 0 \pmod{p^2}.$$

---

* Jour. für Math., 115, 1895, 295-300.

† Quar. Jour. Math., 32, 1901, 1-27, 240-251.

‡ Messenger Math., 30, 1900-1, 78; Proc. London Math. Soc., 33, 1900-1, 49.

§ Math. Annalen, 60, 1905, 471-90; Comptes Rendus, Paris, 142, 1906, 35-8.

|| Proc. London Math. Soc. (2), 4, 1906, 131-5.

¶ Jour. für Math., 135, 1909, 146-156.

** Report British Assoc., 1910, 530; l'intermédiaire des math., 18, 1911, 47; 19, 1912, 159; 20, 1913, 206.

†† Sitzungs. Ak. Berlin, 1913, 663-7.

‡‡ Jour. für Math., 142, 1913, 41-50.

¶¶ Annals of Math., Vol. 18, 1917, 112.